STRATEGY INTERNATIONAL

CYBER READINESS IN PRACTICE

POST TRAINING REPORT

E-Training delivered by:
Focal Point srl
Organized and Powered by Strategy International (SI)

TRAINING REPORT

All content included in this publication is the property of
Strategy International (SI) Ltd.

Protected from the copyright laws of the Republic of Cyprus and international copyright laws.



Strategy International (SI) Ltd, Copyright ©2022-2027

Strategy International (SI) Ltd is a registered company HE423632 In the Republic of Cyprus

The logo of Strategy International is a registered trademark in the Republic of Cyprus. The trademark and works of strategy international (SI) Ltd and its logo are applied for class 31 & 45, in the Republic of Cyprus and EU IPO office.

Cyprus copyrights are governed by the Copyright Section of the Department of the Registrar of Companies and Official Receiver.

The governing laws are: N.63/77, N.18(I)/93, N.54(I)/99, N.12 (I)/2001, N.128 (I)/2002, N.128 (i) 2004 and N.123 (I) 2006.

Copyright protection vests automatically in the Republic of Cyprus.

First Published February/March 2026
Address: 24 Strovolos Str. 2042 Nicosia Cyprus

This publication is the exclusive property, including copyrights, of Strategy International (SI) Ltd. This is the result of a collaboration. A report of the webinar venew recently completed by Focal Point and Strategy International (SI).

This publication in its complete form, or any parts of it, may not be reproduced, duplicated, copied, sold, resold, visited, or otherwise exploited for any commercial purpose. For all purposes, there is a need for a first written consent of the author and the legal representative of Strategy International (SI) Ltd.

SI trademark(s) may not be used in connection with any product or service and publication that has not been given any prior written consent first.

The document produced is endorsed, is its scientific value, and credits are provided to the author.

The editorial Team of
Strategy International (SI) Ltd.

Marketing Team: Rebel Online

Executive Summary

Cyber Readiness in Practice

30 January 2026 | Organised by Strategy International in collaboration with Focal Point srl.

The webinar Cyber Readiness in Practice, held on 30 January 2026 and organised by Strategy International with the participation of trainers from Focal Point srl, convened practitioners and stakeholders to examine the operational dimensions of cyber preparedness in contemporary organisational environments.

The session addressed the recurring discrepancy between documented preparedness—often reflected in certification processes, compliance mechanisms, and policy-based risk management frameworks—and the actual performance of organisations during live cyber incidents. Participants discussed how institutional readiness, when assessed primarily through formal audits or standards-based benchmarks, frequently represents a static assessment that may not adequately reflect an organisation's capacity to respond effectively under real-time adversarial pressure.

Speakers emphasised that cyber-attacks increasingly unfold as prolonged and adaptive campaigns rather than discrete or episodic events. As such, response effectiveness is influenced not only by technical safeguards but also by organisational coordination, leadership decision-making processes, interdepartmental communication, and human cognitive responses in high-stress environments.

In this context, the discussion highlighted the need to transition from compliance-oriented models of cyber resilience towards decision-focused preparedness approaches. Particular attention was given to the value of team-based, adversary-informed training methodologies supported by realistic cyber range environments. These simulation platforms—designed to replicate live network infrastructures and evolving threat scenarios—enable organisations to stress-test operational protocols, enhance situational awareness, and build measurable response capabilities.

The webinar concluded by underscoring the importance of continuous, experience-based training cycles as a critical component of institutional cyber readiness, enabling organisations to strengthen adaptive capacity and improve resilience across complex and evolving threat landscapes

Acknowledgments

On Behalf of Team Strategy International (SI), We would like to formally acknowledge the valuable contributions of the trainers from Focal Point srl, Mr. Christos Grigoriadis and Mr. Christos Lazaridis, who delivered an insightful and practice-oriented presentation on the critical importance of cyber readiness in contemporary organisational environments. Furthermore, the successful organisation of the webinar was made possible through the dedicated efforts of colleagues at Strategy International, notably Ms. Katrien Maes, Head of Business Development and Events, Ms. Emily Wallerstrom, Public Affairs & Communication and the writer of this current report, and Ms. Theofaneia Ntounia, in close collaboration with the leadership of Focal Point srl, Rear Admiral (ret.) Efstathios Kyriakidis and Ms. Natalia Christofi.

On Behalf of Strategy International (SI) team,

Professor Dr. Marios P. Efthymiopoulos
Director & Co-Founder
Strategy International (SI)

Professor of International Security & Strategy
Vytautas Magnus University (VDU), Kaunas, Lithuania

Table of Contents

Executive Summary 3
Acknowledgments 4
Table of Contents 5
Introduction 6
The Reality Check – Why Cyber Readiness Is Overestimated 7
How Attacks Actually Unfold – Understanding Real Adversaries and Real Risk 9
Why Teams Fail Under Pressure – The Human and organizational Gap 11
What Effective Training Must Deliver – From Confidence to Capability 13
From Understanding to Action – Building Readiness Through Realistic Cyber Ranges (Policy Implications) 15
Concluding Remarks 16

Introduction

Cyber security has emerged as a strategic priority for organisations across all sectors. In response to evolving regulatory frameworks and increasing digital interdependence, many institutions have invested substantially in policies, control mechanisms, certification processes, and technical safeguards intended to demonstrate preparedness and risk mitigation. While such measures often contribute to a sense of institutional confidence, recent high-profile cyber incidents across industries indicate that formal compliance and documented procedures do not necessarily translate into effective operational response during real-time crises.

The webinar Cyber Readiness in Practice examined the critical gap between perceived cyber preparedness and actual organisational performance in the face of live incidents. Bringing together professionals from diverse sectors, the session provided a platform to reflect on why organisations that appear resilient in formal assessments frequently encounter significant challenges when responding under operational pressure.

A central premise of the discussion was that cyber incidents should not be understood solely as technical failures, but rather as complex organisational and decision-making challenges. Although governance frameworks, technical tools, and policy instruments are essential components of preparedness, they cannot in themselves ensure an effective response when uncertainty, time constraints, and competing priorities converge. As emphasised by the presenters, cyber incidents do not generate vulnerabilities; instead, they reveal pre-existing deficiencies in coordination, situational awareness, and institutional readiness.

Structured across five thematic sections, the webinar addressed how readiness is frequently overestimated, how adversarial campaigns unfold in practice, why response teams may fail under pressure, what constitutes meaningful and effective training, and how realistic cyber range environments can support safe yet rigorous preparedness testing. This report synthesises the key insights derived from each section and outlines their broader implications for organisational practice and policy development.

The Reality Check – Why Cyber Readiness Is Overestimated

Many organizations operate under the assumption that cyber readiness is achieved once policies are in place, controls are defined, processes are documented, and governance intent is verified. Certifications and audits reinforce this perception by confirming that required standards have been met and that basic security frameworks are in place. As a result, these mechanisms are frequently treated as reliable indicators that cyber risks are being effectively managed.

However, certifications represent only a snapshot in time. Audits are conducted on fixed dates, while organizational environments are constantly changing. New systems are introduced, cloud services expand, identities multiply, and third-party access grows. Temporary exceptions made to accommodate operational needs often become permanent features of the environment. Meanwhile, documentation struggles to keep pace with these changes, gradually losing its connection to day-to-day practice.

This disconnect is especially pronounced in modern hybrid environments. Automation, software-as-a-service platforms, identity sprawl, and outsourced infrastructure create complex and interconnected ecosystems that are constantly adapting. Over time, the original security architecture may no longer reflect how systems are actually configured or used. What appears compliant in documentation may therefore differ significantly from operational reality.

Organizational behavior also changes once certification has been achieved. In the period leading up to audits, teams tend to focus closely on alignment with documented controls. After certification, operational priorities reassert themselves. Pressure to maintain continuity, meet deadlines, and support business objectives increases, and incentives shift accordingly. In this context, controls are rarely abandoned outright. Instead, they are gradually adjusted, weakened, or bypassed to accommodate immediate needs. In practice, controls bend rather than break.

A simple example discussed was password policy. While formal rules may require strong authentication, real-world conditions can lead to shared credentials, multi-factor authentication fatigue, emergency accounts, and access shortcuts. These practices may appear reasonable under pressure but create structural vulnerabilities.

Current regulatory and compliance regimes do not adequately capture this operational gap. Frameworks in Europe, the United States, the Middle East, and Asia largely emphasize the existence of policies, controls, and governance processes. They assess whether organizations can demonstrate compliance, rather than how those controls perform under stress. As a result, formal assurance remains largely static, while risk remains dynamic.

As a result, when incidents occur, organizations often face conflicting dashboards, unclear ownership, delayed escalation, and surprise at unexpected developments. Teams often find themselves saying, “We did not expect this,” despite having passed multiple audits. The central question raised by the webinar is therefore not whether controls exist, but how they function when exposed to real operational pressure. To answer this question, it is necessary to understand how attackers operate in practice and how incidents actually unfold.

How Attacks Actually Unfold – Understanding Real Adversaries and Real Risk

The webinar emphasised that cyber attacks should not be understood as isolated technical incidents, but as extended and deliberate campaigns. Rather than beginning with a clearly identifiable breach, most attacks unfold gradually, often over weeks or months. Their early stages are intentionally quiet and ambiguous. Defenders rarely observe a single, obvious starting point. Instead, they encounter fragmented and incomplete signals that are difficult to interpret in isolation.

To explain how attackers operate in practice, the presenters introduced the MITRE ATT&CK framework as a useful model for understanding adversary behaviour. Within this framework, tactics represent the strategic objectives of attackers, while techniques describe the specific methods they may use to achieve them. Importantly, the framework highlights that attackers do not follow fixed patterns. Instead, they continuously adapt their techniques in response to defensive measures, changing their approach as circumstances evolve.

A central challenge in early detection is that initial attack signals are weak by design. Attackers frequently rely on legitimate credentials, built-in system tools, and low-noise discovery methods that resemble normal user activity. These techniques allow them to operate without causing visible disruption. As a result, their presence blends into everyday system behaviour and is difficult to distinguish from routine operations.

Detection is further complicated by the limited context available to defenders. Security teams are often faced with large volumes of alerts that compete for attention. The severity of individual signals may be unclear, and incomplete information makes interpretation difficult. In such conditions, confirmation bias can emerge, leading teams to assume that unusual activity is benign, temporary, or unrelated to a broader threat.

Attackers exploit this uncertainty by adapting dynamically to defensive responses. When one access route is blocked or detected, alternative pathways are explored. Defensive actions therefore generate feedback loops that attackers can observe and respond to, enabling them to refine their tactics over time. In many cases, this adaptive advantage allows adversaries to remain active within networks despite security controls.

The webinar stressed that not every adversary is relevant to every organization. Attacker interest is shaped by sector, geography, technology, and business model. Critical infrastructure operators, for example, face distinct risks due to high availability requirements, the convergence of operational and information technology, and the public and political sensitivity of service disruptions. These factors make them attractive targets for extortion and disruption campaigns.

Regional threat patterns further illustrate this variation. In Europe, ransomware campaigns targeting essential services are particularly prominent. In the United States, attackers frequently focus on sectors such as energy, healthcare, and transport. In the UAE, supply-chain and strategic infrastructure attacks are more common, while in Japan, advanced persistent campaigns with long dwell times are frequently observed. These patterns reflect differences in economic structure, regulatory environments, and geopolitical context.

Publicly available sources, including ransomware monitoring platforms, provide concrete examples of these dynamics. They document multi-stage intrusions, prolonged periods of undetected access, and delayed containment. Such cases demonstrate how attackers exploit early uncertainty and organizational hesitation to deepen their presence within targeted systems.

In this context, effective threat intelligence requires a shift from general awareness to practical relevance. Organizations benefit more from identifying a limited number of well-understood adversaries with clear objectives than from attempting to monitor a broad range of generic threats. Understanding likely attack paths and pressure points enables more focused and meaningful preparation.

However, many training programs fail to reflect this reality. Generic, scenario-agnostic, and tool-focused exercises often lack adversary context and strategic depth. Without realistic representations of how attacks unfold in practice, such simulations do little to prepare teams for the complexity and ambiguity of real campaigns.

Why Teams Fail Under Pressure – The Human and organizational Gap

Despite having skilled personnel and advanced technical tools, many organizations struggle to manage cyber incidents effectively. As highlighted during the webinar, failure rarely begins with technology itself. In most cases, security systems function as intended, alerts are generated, and relevant data is available. Yet, despite this apparent readiness, response efforts often deteriorate as incidents unfold.

This is because cyber incidents are fundamentally decision problems rather than purely technical challenges. Teams are required to act on incomplete and uncertain information, under significant time pressure, while balancing operational continuity, legal obligations, reputational concerns, and financial risk. In such circumstances, technical expertise alone is insufficient. What matters most is the ability to prioritise, coordinate, and make timely judgements in uncertain conditions.

One of the first effects of an unfolding incident is cognitive overload. As activity increases, alert volumes rise sharply and information becomes fragmented across multiple systems and teams. Individual attention is limited, and as pressure intensifies, focus tends to narrow. Broader situational awareness declines, making it difficult to maintain a clear overview of what is happening and why.

Although modern security environments generate vast quantities of data, more information does not automatically lead to better understanding. Telemetry from different sources often requires manual correlation, and meaningful patterns may only become visible after significant delay. Teams may therefore find themselves surrounded by data without a coherent interpretation of events. This gap between data and understanding can delay decisive action.

Organizational structures further complicate response efforts. Decision-making authority is not always clearly defined, and uncertainty about responsibility can lead to hesitation. Escalation pathways may be slow, and cross-team dependencies create additional bottlenecks. Legal, compliance, communications, and technical functions often operate according to different priorities and timescales, making coordination more difficult precisely when speed is essential.

Leadership pressure also plays a significant role in shaping behavior. Senior management frequently seeks certainty and aims to minimize operational disruption. While understandable, this emphasis can discourage early containment measures that may appear disruptive in the short term. As a result, teams may postpone decisive action in order to avoid visible impact, even when delay increases long-term risk.

Communication challenges further undermine effective response. Technical assessments do not always translate clearly into business implications, and non-

specialist stakeholders may struggle to interpret complex security information. At the same time, status updates are sometimes framed to reassure senior leadership rather than to convey uncertainty and risk. This can lead to misaligned expectations and delayed decision-making.

Fear of being wrong is another powerful influence. In high-pressure situations, teams are often reluctant to escalate incidents or isolate systems without complete confirmation. This tendency towards over-validation reflects a desire to avoid unnecessary disruption or criticism. However, it also contributes to delayed containment and wider impact.

Traditional training approaches do little to prepare teams for these realities. Exercises are often conducted in calm, predictable environments with known outcomes and limited consequences. Such scenarios do not reproduce the stress, ambiguity, and organizational tension of real incidents. As a result, participants may perform well in training while remaining unprepared for genuine crises.

When real incidents occur, these limitations become apparent. Organizations discover that key decisions have not been practiced, roles are poorly defined, and coordination must be improvised. These shortcomings do not reflect individual incompetence, but rather inadequate preparation models that fail to reflect operational reality. The webinar therefore argued that improving incident response requires addressing human and organizational factors as seriously as technical capability.

What Effective Training Must Deliver – From Confidence to Capability

Given that cyber incidents are fundamentally decision problems shaped by pressure and uncertainty, the presenters argued that existing training approaches must be reconsidered. Simply acquiring technical knowledge or becoming familiar with specific tools does not guarantee effective performance during real crises. Traditional cyber training typically relies on static scenarios, predetermined outcomes, tool-centred exercises, and individual assessment. While such methods may improve technical competence, they tend to build confidence rather than genuine operational capability.

Effective training, the webinar emphasised, must focus on validating decisions rather than merely rehearsing actions. Participants need opportunities to practise prioritising tasks, determining which risks are acceptable, and deciding what issues can be deferred. These judgements are central to incident response but are rarely tested in conventional exercises. Without regular exposure to such decision-making challenges, teams may struggle to act decisively when real incidents occur.

To support this objective, training environments must reflect the complexity of operational systems. Realistic telemetry and background noise are essential. Participants should be required to interpret imperfect alerts, conflicting signals, and ambiguous evidence, rather than relying on clear and unambiguous indicators. Exposure to uncertainty helps teams develop the analytical discipline needed to operate effectively under pressure.

The presenters also highlighted the importance of team-based training. Incident response is not an individual activity but a coordinated organisational effort. Exercises should therefore involve security analysts, detection engineers, system administrators, offensive and defensive specialists, and decision-makers. By working together in simulated incidents, participants can practise communication, coordination, and shared responsibility, all of which are critical during real crises.

Training scenarios must also align with realistic adversary behaviour. Generic simulations that lack strategic context fail to reflect how real attackers operate. More effective exercises are built around adaptive techniques and objective-driven campaigns that evolve in response to defensive actions. Such scenarios encourage participants to think strategically rather than mechanically, reinforcing the need to anticipate and respond to changing threats.

Repetition and iteration were identified as central to building sustained capability. One-off exercises, regardless of their quality, cannot establish long-term readiness. Repeated training sessions expose persistent weaknesses, allow progress to be tracked, and introduce new challenges over time. Through iteration, organisations can move from isolated learning experiences to continuous capability development.

Meaningful measurement is also essential. Rather than focusing solely on technical performance, organisations should assess operational indicators such as time to detection, time to response, realism of detection coverage, and quality of cross-team coordination. These metrics provide insight into how effectively teams function under pressure and where further improvement is needed.

Finally, the presenters stressed that training must support learning as well as performance. Instructor guidance, structured reflection, and systematic after-action analysis enable participants to understand why decisions were made, what worked, and what did not. Without these processes, valuable lessons may be lost, and exercises risk becoming routine activities rather than opportunities for improvement.

From these elements, the webinar derived a set of core training principles. Effective programmes should be:

- Decision-centric
- Adversary-informed
- Team-based
- Iterative
- Measurable

By embedding these principles into their training strategies, organisations can move beyond symbolic preparedness and towards demonstrable operational capability.

From Understanding to Action – Building Readiness Through Realistic Cyber Ranges (Policy Implications)

The final section of the webinar addressed a fundamental implementation challenge: how organizations can apply effective training principles in practice without exposing operational systems to unacceptable risk. While realistic exercises are essential for building readiness, learning through live incidents or experimentation in production environments carries significant financial, legal, safety, and reputational consequences. These risks discourage meaningful testing and reinforce conservative, risk-averse behavior.

To overcome this limitation, the presenters highlighted the role of cyber ranges as a practical enabling mechanism. By providing isolated, controlled, and repeatable environments, cyber ranges allow organizations to simulate realistic incidents without endangering critical services. Within these environments, teams are free to experiment, make mistakes, and explore alternative responses, conditions that are rarely possible in live systems.

However, the webinar emphasized that generic training platforms offer limited strategic value. Simplified infrastructures and standardized scenarios do not reflect the operational realities of complex organizations. Effective readiness validation requires sector-specific and organization-specific modelling. Training environments must replicate real architectures, dependencies, regulatory constraints, and operational priorities in order to generate meaningful insights.

This tailored approach enables organizations to move beyond abstract preparedness and towards evidence-based assurance. Through repeated exercises in realistic environments, institutions can observe how their systems, teams, and leadership structures perform under pressure. Over time, patterns emerge that reveal both strengths and persistent vulnerabilities. These findings provide a concrete basis for improvement rather than reliance on assumptions or external certification alone.

From a policy and governance perspective, this shift has important implications. Traditional oversight frameworks place strong emphasis on compliance, documentation, and periodic audits. While these mechanisms remain necessary, they are insufficient indicators of operational resilience. The webinar argued that governance models should increasingly prioritize demonstrated capability, supported by structured training evidence and measurable performance indicators.

This approach encourages leadership to treat cyber readiness as a continuous organizational process rather than a periodic compliance exercise. Investment decisions, risk assessments, and regulatory reporting can be informed by observed performance in controlled environments, rather than by static documentation. In this

way, training becomes an integral component of risk management and strategic planning.

Concluding Remarks

The concluding message of the current webinar was that effective cyber resilience cannot be achieved through formal structures alone.

It must be built through repeated testing, realistic simulation, and honest evaluation of organizational behavior under pressure.

Cyber ranges provide the infrastructure for this process, but their value depends on thoughtful design, sector relevance, and sustained institutional commitment.

STRATEGY INTERNATIONAL

24 Minoos Str., Strovolos, Nicosia,
2042 Cyprus
info@strategyinternational.org
https://strategyinternational.org/